

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA**

<hr/>)	
<i>Beach, et al.,</i>)	Case No. 13-185 (JNE/TNL)
)	
v.)	
)	
<i>Hunt, et al.</i>)	
<hr/>)	Case No. 13-389 (JNE/TNL)
<i>Davis-Dowling, et al.,</i>)	
)	
v.)	
)	
<i>Hunt, et al.</i>)	
<hr/>)	
<i>Sapp, et al.,</i>)	Case No. 13-286 (JNE/TNL)
)	
v.)	
)	
<i>Hunt, et al.</i>)	
<hr/>)	
<i>Whigham, et al.</i>)	Case No. 13-208 (JNE/TNL)
)	
v.)	
)	
<i>Hunt, et al.</i>)	
<hr/>)	
<i>Kiminski et al.</i>)	Case No. 13-358 (JNE/TNL)
)	
v.)	
)	
<i>Hunt, et al.</i>)	
<hr/>)	

**STATE DEFENDANTS' MEMORANDUM
IN SUPPORT OF THEIR MOTION TO DIMISS**

INTRODUCTION

In late 2012, the Minnesota Department of Natural Resources (“DNR”) discovered that one of its law enforcement employees, John Hunt, had viewed drivers’ license data without a proper purpose. The DNR investigated, terminated Hunt’s employment, referred him for criminal prosecution, and disclosed to the affected people, including the Plaintiffs, Hunt’s unlawful access of their drivers’ license information.

The Plaintiffs have filed five related putative class actions seeking damages from John Hunt. The Plaintiffs allege that Hunt is liable for violations of the Driver’s Privacy Protection Act (“DPPA”), 18 U.S.C. § 2721 *et seq.*, and their constitutional right of privacy. The Plaintiffs additionally sue ten other named state government officials or employees (the “State Defendants”) and State Doe defendants,¹ alleging they are personally liable to pay over \$12.5 million in damages to the Plaintiffs for Hunt’s actions.

The Plaintiffs do not allege that any of the State Defendants personally accessed or disclosed the Plaintiffs’ drivers’ license data. Instead, they seek to hold the State Defendants liable for supervising Hunt, or for creating or maintaining the database that

¹ The Plaintiffs name John and Jane Doe defendants, but do not plead sufficient detail to identify who they are, or if they even exist. The Plaintiffs’ allegations of conduct by the Doe defendants are, in character, the same as the Plaintiffs’ allegations of conduct by State Defendants. As a result, if the Court dismisses the State Defendants, it should also dismiss the Doe defendants.

Hunt improperly accessed. Neither the DPPA nor the constitutional right of privacy make government officials liable for simply supervising bad actors, or for creating or maintaining a database illegally accessed by other people. As a result, the Plaintiffs' claims against the State Defendants should be dismissed in their entirety.

BACKGROUND

The Plaintiffs bring five suits as putative class actions, alleging a right of recovery for the improper viewing of drivers' license data by defendant Hunt. (Consol. Compl. ¶¶ 30-36.) Defendants Tom Landwehr and Ramona Dohman are the current Commissioners of the DNR and Minnesota Department of Public Safety ("DPS"), respectively, and are sued in their individual and official capacities. (*Id.* ¶¶ 20, 26.) Defendants Mark Holsten and Michael Campion are the immediately preceding Commissioners of the DNR and DPS, respectively, and also are sued in their individual capacities. (*Id.* ¶¶ 21, 25.) Defendants Keith Parker, Robert Maki, Steve Lime, Charlie Regnier, Stan Gruska, and Sheila Deyo are employees of the DNR or Minnesota Office of Enterprise Technology who work for or provide services to the DNR. (*Id.* ¶¶ 17-19, 22.) They are sued in their individual capacities. (*Id.*) The Plaintiffs also purport to sue Doe defendants working for DPS. (*Id.* ¶¶ 27-28.)

The present versions of the complaints filed in the five related actions are identical with the exception of naming different plaintiffs. Because the lawsuits vary in the number of named plaintiffs, the paragraph numbering of each complaint also varies. For

the purposes of this memorandum, references to the consolidated complaint are to the complaint filed in *Beach v. Hunt*, Case. No. 13-185.

ARGUMENT

I. THE PLAINTIFFS FAIL TO STATE A CLAIM UNDER THE DPPA.

The Plaintiffs have a right of relief under the DPPA, but it is not against the State Defendants. It is against John Hunt. The DPPA does not make the State Defendants liable for Hunt's actions. Nor does the DPPA make the State Defendants liable for alleged negligence or misfeasance in creating or maintaining a drivers' license database that is essential to the State's law enforcement activities. To hold otherwise would be contrary to the plain language of the DPPA, as well as the purpose and intent of the act.

A. Background Of The DPPA.

The DPPA was passed in 1994 in response to the murder of actress Rebecca Schaefer by a stalker who had obtained her unlisted home address from the California Department of Motor Vehicles. Maureen Maginnis, *Maintaining the Privacy of Personal Information: The DPPA and the Right of Privacy*, 51 S.C. L. Rev. 807, 809 (2000).

Congress enacted the DPPA to prevent persons from knowingly obtaining, disclosing or using drivers' license data for improper purposes, and included a long list of permitted purposes for which access is allowed. For example, the DPPA permits disclosure of drivers' license data to government agencies, auto dealers, civil litigants, academic researchers, insurers, private investigators, and many others. 18 U.S.C. § 2721(b). As originally passed, the DPPA even permitted disclosure to direct marketing firms unless the driver specifically opted out. Maginnis, *supra*, 51 S.C. L. Rev. at 809-

10. The DPPA was only later amended to require the subject of the data to “opt-in” before a disclosure to direct marketers could be made. *Id.* The DPPA additionally permits States to sell drivers’ license data to third parties such as Westlaw for further dissemination to permitted users. 18 U.S.C. § 2721.

The DPPA does not mandate the manner in which drivers’ license information is stored, handled, maintained, or supervised. There are no implementing federal regulations concerning the handling of drivers’ license data under the DPPA. The absence of such regulations is in stark contrast to other federal privacy statutes. For example, the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and associated regulations contain detailed provisions regulating the storage and transmission of health data, as well as specific oversight requirements for supervisors. *See, e.g.*, 45 C.F.R. § 164.308.²

To effectuate the intent of the act, the DPPA created a limited right of private suit against persons who “knowingly” and improperly obtain, disclose or use drivers’ license data. The DPPA provides that:

A person who *knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter* shall be liable to the individual to whom the information pertains, who may bring a civil action in a United States district court

² Among other things, the HIPPA regulations require that entities in possession of health data conduct risk assessments, implement security measures, audit access to information, and compartmentalize access. 45 C.F.R. § 164.308.

18 U.S.C. § 2724 (emphasis added). States and State agencies are specifically exempted from the definition of “persons” who may be privately sued. 18 U.S.C. § 2725(2). Instead, the DPPA confers the exclusive authority on the United State Attorney General to take action against State departments of motor vehicles. As the DPPA states:

Any State department of motor vehicles that has a policy or practice of substantial noncompliance with this chapter shall be subject to a civil penalty imposed by the *Attorney General* of not more than \$5,000 a day for each day of substantial noncompliance.

18 U.S.C. § 2723 (emphasis added).

B. The State Defendants Are Not Liable For John Hunt’s Misuse Of The Plaintiffs Drivers’ License Data.

The Plaintiffs’ claims are predicated on the misplaced argument that the State Defendants can be held liable for John Hunt’s misuse of their drivers’ license data merely because the State Defendants failed to stop it. *See, e.g.*, Consol. Compl. ¶¶ 57-58. These allegations do not state a claim under the DPPA, which imposes liability only if the defendant “knowingly obtains, discloses or uses” such data for a “purpose not permitted” by the act. 18 U.S.C. § 2724. The State Defendants must therefore be dismissed.

1. The Plaintiffs have not pled a cause of action against any State Defendant.

As discussed above, the narrow private cause of action under the DPPA applies to “[a] person who *knowingly obtains, discloses or uses* personal information, from a motor vehicle record, *for a purpose not permitted under this chapter.*” 18 U.S.C. § 2724 (emphasis added). The Plaintiffs do not allege any act by any State Defendant that falls within the limited scope of this provision. Indeed, the Plaintiffs do not allege that any

State Defendant personally obtained, disclosed, or used drivers' license data, let alone for a "purpose not permitted."

At best, the Plaintiffs allege that the State Defendants created and maintained a database of drivers' license data that Hunt misused. (*See, e.g.*, Consol. Compl. ¶¶ 36-37.) But the creation or maintenance of drivers' license databases is not actionable under the DPPA. Congress knows how to craft and enact statutes that impose liability for improperly maintaining information. As noted above, Congress did so, for instance, with health information through HIPAA. *See supra* n.2. Congress did not do so in the DPPA. Instead, it chose to create a limited private cause of action to impose liability only for the wrongful act of actually obtaining, disclosing, or using drivers' license data for an improper purpose, and exempt States and state agencies from a private cause of action. 18 U.S.C. §§ 2723, 2724.

This Congressional intent is also reflected in section 2723 of the DPPA, which empowers only the United States Attorney General to bring an enforcement action against State departments of motor vehicles. The Attorney General's authority is limited to sanctioning conduct of a State which constitutes "a policy or practice of substantial noncompliance with [the DPPA]" 18 U.S.C. § 2723(b). The only remedy of the Attorney General is to impose a civil penalty of "not more than \$5,000 a day for each day of substantial noncompliance," *id.*, not the various actual, liquidated, or punitive damages and other remedies available to private litigants against the person who actually

“knowingly obtains, discloses or uses” drivers’ license information for an improper purpose. 18 U.S.C. § 2724.

To the extent the Plaintiffs allege that the State Defendants are liable merely because they knew Hunt had access to the State’s drivers’ license database, even if they were unaware of his improper use of the data (*see, e.g.*, Consol. Compl. ¶ 80), such allegations cannot sustain a private right of action under the DPPA. To hold otherwise would make State officials strictly liable for the misdeeds of any person who misuses drivers’ license data obtained from the State. The results would be catastrophic, particularly if statutory liquidated damages of \$2,500 per violation are imposed. The Court should not presume that Congress intended such an absurd result, particularly where other federal statutes that impose liability for mismanagement of data do so in clear and unambiguous terms. *See City of Jefferson City, Mo. v. Cingular Wireless, LLC*, 531 F.3d 595, 606 (8th Cir. 2008) (holding federal courts assume legislatures do not intend absurd results when passing statutes); *Foulk v. Charrier*, 262 F.3d 687, 703 (8th Cir. 2001) (same).

In Minnesota alone, drivers’ license data is accessed thousands of times per day for legitimate purposes. If the DPPA made State officials liable for every misuse of the database by others, State officials may be left with the impossible choice of either shutting down the database or running the risk of ruinous personal liability. Rather, Congress carefully crafted limited remedies under the DPPA that:

- Created a narrow private cause of action which imposes liability only on individuals or entities that personally obtain, disclose, or use drivers' license data without proper purpose;
- Exempted States and State agencies from private suits for damages;
- Did not impose private liability for oversight of the drivers' license database; and
- Empowered only the U.S. Attorney General to impose a limited civil penalty against State departments of motor vehicles that engage in conduct that constitutes "a policy or practice of substantial noncompliance."

18 U.S.C. §§ 2723, 2724.

As private litigants, the Plaintiffs must therefore plead and prove that the State Defendants personally obtained, used, or disclosed the Plaintiffs' drivers' license data for an improper purpose. They have not and cannot meet this burden.

2. Even if relevant, the Plaintiffs have not sufficiently pled that any State Defendant knew of Hunt's misuse of the drivers' license database.

In support of their allegations that the State Defendants mismanaged access to the drivers' license database, the Plaintiffs plead that the State Defendants "knew" of Hunt's misuse, and did nothing to stop it. *See, e.g.*, Consol. Compl. ¶¶ 53, 54. Even assuming that knowledge of Hunt's improper actions would support a private right of action under the DPPA against the State Defendants as opposed to civil penalties imposed by the Attorney General, the Plaintiffs have not sufficiently pled facts to support their allegations that the State Defendants knew of Hunt's misuse.

In *Bell Atlantic v. Twombly*, 550 U.S. 544 (2007) and *Ashcroft v. Iqbal*, 556 U.S. 662 (2009), the Supreme Court abrogated its prior case law on pleading standards, holding that plaintiffs can no longer survive a motion to dismiss with pleadings that

simply “[leave] open the possibility that [the] plaintiff might later establish some set of undisclosed facts to support recovery.” *Twombly*, 550 U.S. at 561. The Supreme Court now requires plaintiffs to plead facts that “allow[] the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Iqbal*, 556 U.S. at 678. The purpose of the Supreme Court’s shift in pleading standards is to make clear that notice pleading under Rule 8 “does not unlock the doors of discovery for a plaintiff armed with nothing more than conclusions.” *Id.*

Here, the Plaintiffs employ the exact type of pleading barred by *Twombly/Iqbal* in making only conclusory allegations that the State Defendants “knew” of Hunt’s unauthorized accessing of the drivers’ license database. The Plaintiffs attempt to support these conclusory allegations with assertions that are nothing more than purported biographical information regarding the Commissioner Defendants. (*See, e.g.*, Consol. Complaint ¶¶ 82-91.) These allegations do not show knowledge of John Hunt’s impermissible use of drivers’ license data. In addition, with respect to the non-Commissioner and Doe State Defendants, the Plaintiffs allege nothing at all beyond a bare allegation that they knew of Hunt’s conduct. (Consol. Compl. ¶¶ 53, 54.) As *Iqbal* held, “[t]hese bare assertions, much like the pleading of conspiracy in *Twombly*, amount to nothing more than a ‘formulaic recitation of the elements’ of a constitutional discrimination claim, As such, the allegations are conclusory and not entitled to be assumed true.” 556 U.S. at 681-82 (quoting *Twombly*, 550 U.S. at 555).

Iqbal empowers the Court to review the claims of misconduct made by a plaintiff in light of more likely, and less sinister, explanations. *Iqbal*, 556 U.S. at 682. It also requires the Court to reject the Plaintiffs' claims if not supported by specific factual allegations that convert conclusory assertions from merely conceivable to plausible. *Id.* In this case, the Plaintiffs' conclusory allegations do not overcome the plausible explanation that Hunt was a rogue employee who violated the policies of the DNR and DPS until he was caught and fired.

Indeed, the Plaintiffs' own allegations support the conclusion that Hunt's unlawful activities were not authorized, condoned or otherwise known by the State Defendants.

As the Plaintiffs plead:

- The DNR terminated Defendant Hunt after his unlawful access of the Plaintiffs' drivers' license data was discovered. (Consol Compl. ¶ 43.)
- The DNR publicly disclosed the data breach and communicated with the affected persons. (Consol. Compl. ¶¶ 44-49.)
- In those communications, the DNR stated that Hunt's actions were "unauthorized" and "inappropriate." (Consol. Compl. ¶¶ 46-48.)
- In addition, as earlier versions of the Plaintiffs' complaints pled, Hunt was criminally charged for his unlawful access. (*Ness/Beach* Compl. ¶ 44; *Whigham* Compl. ¶ 53; *Downing* Compl. ¶ 25.)

The Plaintiffs therefore plead the implausible claim that the very same people who uncovered Hunt's unlawful access, terminated his employment, referred him for criminal prosecution, and revealed the data breach to the victims, knowingly conspired with Hunt. The Plaintiffs fail to plead any facts rendering this claim plausible, and the Court should therefore also dismiss claims against the State Defendants based on *Twombly/Iqbal*.

II. THE PLAINTIFFS FAIL TO STATE A CLAIM UNDER THE CONSTITUTIONAL RIGHT OF PRIVACY.

The Plaintiffs plead two counts (IV and V) against the State Defendants based in whole or part on alleged violations of the constitutional right of privacy. These claims should be dismissed because the Plaintiffs cannot even meet the threshold requirement of showing that drivers' license data is the type of intimate information protected from disclosure by the constitutional right of privacy.

Right of privacy claims rarely rise to the level of a constitutional violation. *Alexander v. Pfefer*, 993 F.2d 1348, 1350-51 (8th Cir. 1993). As the *Alexander* court held:

As a preliminary matter we note that tortious conduct even when performed under the color of law does not become a constitutional wrong. "[T]he personal rights found in [the] guarantee of personal privacy must be limited to those which are 'fundamental' or 'implicit within the concept of ordered liberty.'"

Just last term, the Supreme Court reaffirmed its reluctance to expand its concept of substantive due process "because guideposts for responsible decision making in this uncharted area are scarce and open-ended."

[We] have previously rejected claims that the Due Process Clause should be interpreted to impose federal duties that are analogous to those traditionally imposed by state tort law.

Alexander, 993 F.2d at 1350 (citing *Paul v. Davis*, 424 U.S. 693 (1976) and *Collins v. City of Harker Heights, Tex.*, 503 U.S. 115, 125 (1992)).

As a result, federal courts have dismissed constitutional privacy claims in all but the most extreme cases involving highly sensitive information. Drivers' license data does not meet this standard. *Collier v. Dickinson*, 477 F.3d 1306, 1308 (11th Cir. 2007) (holding that a release of drivers' license data did not constitute a constitutional right of privacy claim). Individuals show drivers' licenses to prove identity in a myriad of situations – when entering a bar, when cashing a check, when boarding a plane. Given the frequency with which drivers' license data is requested and provided on a day-to-day basis, the disclosure of such information cannot rise to the level of a constitutional violation.

Indeed, federal courts have dismissed cases involving information far more sensitive than drivers' license information. In *Alexander*, the defendant sheriff revealed in a radio interview that the plaintiff had failed to qualify to become an officer. *Alexander*, 993 F.2d at 1349. In *Davis III v. Bucher*, 853 F.2d 718 (9th Cir. 1988), the defendant prison guard circulated nude photographs of an inmate's wife. *Id.* at 719. In *Lambert v. Hartman*, 517 F.3d 433 (6th Cir. 2008), the defendant clerk of court posted the plaintiff's social security number on the internet, resulting in an identity theft. *Id.* at 435. In each of these cases the courts found that the information was not sufficiently sensitive to be a basis for a constitutional violation of the right of privacy. This Court should similarly dismiss the Plaintiffs' constitutional claim.

III. EVEN ASSUMING, ARGUENDO, THAT THE PLAINTIFFS HAVE PLED A CLAIM AGAINST THE STATE DEFENDANTS UNDER THE DPPA OR CONSTITUTIONAL RIGHT OF PRIVACY, THE PLAINTIFFS CANNOT MAINTAIN SUITS FOR DAMAGES BECAUSE THE STATE DEFENDANTS HAVE QUALIFIED IMMUNITY.

As discussed above, the State Defendants did not violate the DPPA or a constitutional right of privacy and therefore they should be dismissed from this case. In the alternative, the Court should dismiss the damages claims against the State Defendants based on the doctrine of qualified immunity.

Qualified immunity shields officials, like the State Defendants, from liability for actions taken under color of law unless their conduct “violate[s] clearly established statutory or constitutional rights of which a reasonable person would have known.” *Pearson v. Callahan*, 555 U.S. 223, 231 (2009). In *Roth v. Guzman*, 650 F.3d 603, 611 (6th Cir. 2011) the Sixth Circuit applied qualified immunity to damages claims against State officials under the DPPA. *Id.* at 612. The Court should do the same in this case because liability under the DPPA, as pled by the Plaintiffs, was not clearly established at the time of the alleged conduct.

The Court should also dismiss the Plaintiffs’ constitutional claims for damages because there is no clear constitutional right of privacy in drivers’ license data. *See Collier*, 477 F.3d at 1308. *See also, e.g., Tokar v. Armontrout*, 97 F.3d 1078, 1084 (8th Cir. 1996) (applying qualified immunity to claim that disclosure of HIV status violated the plaintiff’s constitutional right of privacy); *Bloch v. Ribar*, 156 F.3d 673, 683 (6th Cir. 1998) (applying qualified immunity to claim that disclosure of details of a rape violated the plaintiff’s constitutional right of privacy.)

In *Bloch*, for example, the plaintiffs were a husband and wife who sued a sheriff for holding a press conference in which he disclosed the details of the wife's rape to the media. *Id.* at 676. The plaintiffs alleged that the sheriff made the disclosure in retaliation for the plaintiffs' public criticism of the sheriff's investigation of the crime. *Id.* The court dismissed the plaintiffs' claim because "a reasonable public official would not be on notice that the release of such intimate details of a rape constituted an actionable violation of a rape victim's privacy interests." *Id.* at 686. As a result, the court held that the sheriff was entitled to qualified immunity. *Id.* at 687.

Drivers' license data is far less sensitive than the information disclosed in *Bloch*. Even under the most favorable view of the Plaintiffs' pleading, the State Defendants, unlike the sheriff in *Bloch*, did not intentionally disseminate drivers' license information for impermissible purposes, and certainly did not do so for the purpose of retaliating against the Plaintiffs.

IV. THE PLAINTIFFS' SECTION 1983 CLAIM BASED ON ALLEGED VIOLATIONS OF THE DPPA SHOULD BE DISMISSED.

The Plaintiffs plead DPPA claims in two ways. In Count I, they plead a claim directly under the DPPA. In Counts III and V, they plead a claim under 42 U.S.C. § 1983 for violation of the DPPA. The Court should dismiss the Section 1983 claim

because, as discussed above, the State Defendants did not violate the DPPA.³ *See supra*, Section I. In any event, Section 1983 cannot be used to enforce the DPPA.

Not all federal statutes are enforceable through a Section 1983 action. The DPPA may not be enforced under Section 1983 if Congress implicitly foreclosed use of Section 1983 for that purpose by including remedies in the DPPA that are inconsistent with Section 1983 relief. *See, e.g., Livadas v. Bradshaw*, 512 U.S. 107, 133 (1994) and *Alexander v. Sandoval*, 532 U.S. 275, 290 (2001) (holding that federal statute may not be enforced through a Section 1983 action where the statute includes provisions for relief that are incompatible with Section 1983).

There is a split in authority whether Congress implicitly foreclosed Section 1983 enforcement of the DPPA. *See Roberts v. Source for Pub. Data*, 606 F. Supp. 2d 1042, 1046 (W.D. Mo. 2008) (holding Section 1983 enforcement of the DPPA is implicitly foreclosed); *Kraege v. Busalacchi*, 687 F. Supp. 2d 834 (W.D. Wis. 2009) (same); *Collier v. Dickinson*, 477 F.3d 1306 (11th Cir. 2007) (holding Section 1983 enforcement of the DPPA is not implicitly foreclosed); *Arrington v. Richardson*, 660 F. Supp. 2d 1024 (N.D. Iowa 2009) (same). The Eighth Circuit and the District Court of Minnesota have not addressed the issue. The Court should follow the better reasoned analysis of *Roberts* and *Kraege* and hold that Congress implicitly foreclosed Section 1983 enforcement of the DPPA.

³ Of course, the Section 1983 claim based on an alleged violation of a constitutional right of privacy should also be dismissed because the State Defendants did not violate any

All four cases cited above conduct the same inquiry, analyzing whether the terms of the DPPA are incompatible with enforcement under Section 1983. The *Roberts* and *Kraege* courts correctly concluded that enforcement terms of the DPPA are incompatible with Section 1983. There are at least four ways in which the enforcement provisions of the DPPA are incompatible with enforcement under Section 1983.

First, the DPPA contains criminal penalties, 18 U.S.C. § 2723(a), but Section 1983 does not. Second, unlike Section 1983, the DPPA permits the U.S. Attorney General to enforce the act against States through imposition of civil penalties. 18 U.S.C. §2723(b). Third, the DPPA does not permit a private cause of action against States or State agencies, 18 U.S.C. § 2724(a), 2725, including for injunctive relief, 18 U.S.C. § 2724(b)(4), whereas by use of official capacity suits Section 1983 does effectively permit private parties to sue State agencies for prospective injunctive relief. Indeed, the Plaintiffs seek official capacity prospective injunctive relief in Count V of their complaints. Fourth, even the U.S. Attorney General cannot obtain injunctive relief against a State or State agency under the DPPA. 18 U.S.C. § 2723(b).

Given the express remedial provisions of the DPPA, Congress must have intended for the DPPA to be enforced only through its own terms. The Court should therefore also dismiss the Plaintiffs' Section 1983 claims to enforce the DPPA based on the incompatibility of the DPPA and Section 1983 enforcement provisions.

such right. See *supra*, Section II.

CONCLUSION

For the reasons set forth above, the Court should enter an order dismissing the State Defendants, with prejudice.⁴

Dated: April 30, 2013

Respectfully submitted,

OFFICE OF THE ATTORNEY GENERAL
State of Minnesota

s/ Oliver J. Larson

OLIVER J. LARSON
Assistant Attorney General
Atty. Reg. No. 0392946

JOHN S. GARRY
Assistant Attorney General
Atty. Reg. No. 0208899

JOHN R. MULÉ
Assistant Attorney General
Attorney Reg. No. 0393031

445 Minnesota Street, Suite 1800
St. Paul, Minnesota 55101-2134
(651) 757-1265 (Voice)
(651) 282-2525 (TTY)

ATTORNEYS FOR THE STATE
DEFENDANTS

⁴ As previously referenced, the Doe defendants should also be dismissed. *See supra*, n.1.